MARTHA BOERSCH (CABN 126569)
Attorney for the United States
Acting under Authority Conferred by 28 U.S.C. § 515

MARTHA BOERSCH (CABN 126569)
Chief, Criminal Division

NIKHIL BHAGAT (CABN 279892)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7193
FAX: (415) 436-6982
nikhil.bhagat@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. KEITH LATTERI, Defendant.	Case No. CR 23-471 WHO **GOVERNMENT'S SENTENCING MEMORANDUM** Sentencing Date: May 1, 2025 Sentencing Time: 1:30 p.m. Before: The Honorable William H. Orrick

Pursuant to Local Criminal Rule 32-5(b), the United States of America respectfully submits this sentencing memorandum to aid the Court in its determination of a sentence that is sufficient but not greater than necessary to promote the purposes set forth in the sentencing statute.

The defendant's criminal conduct—hacking into a multinational tech company in an intrusion that lasted months and compromised hundreds of accounts, which allowed him and his co-defendant access into a much larger company—was significant, and caused the companies to suffer millions of dollars in damage.

It was also part of a troubling, years-long pattern in which the defendant terrorized all means of denizens on the Internet, by, among other things, "doxing" them by disclosing their personal

information, Swatting, SIM swapping, unlawfully obtaining live location data, gaining access to personal cloud storage, threatening them, and perhaps most disturbingly, using social engineering to obtain sexually explicit images of underage girls and using those images to blackmail them. Moreover, on at least three occasions, the defendant forged federal court documents in an attempt to shut down Internet sites he did not like.

On the other hand, although it does not excuse his crimes, the defendant has had a particularly difficult upbringing. He was also relatively young at the time of the offense and accepted responsibility quickly.

For the reasons set forth below, the Court should impose a below-guideline sentence of 36 months in the custody of the Bureau of Prisons, followed by three years of supervised release including the special conditions recommended by probation as well as one additional condition discussed below, and restitution of $4,334,530.64.

I. The Offense Was Serious, Caused Millions of Dollars in Damage, and Took Place Over a Sustained Period (*18 U.S.C. § 3553(a)(1)--Nature and Circumstances of the Offense)* [1]

A. Phase One (December 21, 2018 through February 16, 2019)

On the night of December 21, 2018, Latteri and his co-defendant, Noah Roskin-Frazee, unlawfully gained access to the credentials of a high-level employee of COMPANY B. That employee had access to reset the passwords of approximately 3,000 advisor accounts. COMPANY B provides customer experience solutions—as a contractor to other companies, including COMPANY A. COMPANY A, in turn, is a leading U.S.-based multinational provider of computer hardware, tablets, mobile devices, and software.

Using that access, the attackers reset the password of another COMPANY B employee and gained access to COMPANY B's network through that individual. Ultimately, the attackers used this

[1] Unless otherwise stated, the facts stated in this section are drawn from the PSR and Paragraph 2 of the defendant's plea agreement.

COMPANY B employee's access to get into a COMPANY A customer relations tool. That tool allowed the user to access substantial amounts of COMPANY A information, including customer information lookup, repair instructions, customer call logs, chat features, search by device serial numbers, and importantly, the ability to enter orders for replacement hardware without cost.

COMPANY B initially detected suspicious activity on its network on December 24, 2018 and eventually engaged a third-party incident response firm to help. It was not until January 18, 2019, however, that COMPANY B was able to successfully stop the attackers from using this line of attack.

B. Phase Two (January 16, 2019 through February 16, 2019)

But unbeknownst to COMPANY B, Latteri and his co-defendant already had access to another way into COMPANY B's network: the JAMF platform. By deploying a series of scripts on more than 6,000 COMPANY B units, they were able to gain access to an even more powerful COMPANY A tool that not only gave them the ability to send out *replacement* hardware and software without charge, but actually gave them access to a COMPANY A database that allowed them to view and edit orders for COMPANY A hardware and software and electronic gift cards. As described below, Latteri's co-defendant used this access to order more than $100,000 worth of hardware, and an attacker using the same access got away with $2.7 million in COMPANY A gift cards.

The intrusion finally stopped on February 16, 2019, when COMPANY B, working with its incident response team, was able to blacklist the attackers' IP address and take other action to eliminate their access to the system. In total, Latteri and his co-defendant were in the COMPANY B network for six weeks. In total, from the intrusion itself, COMPANY B suffered more than $3.8 million in remediation costs, *see* Plea Agmt., and COMPANY A expended more than $650,000 as a result of the intrusion. *See* Ex. C.

During the intrusion, Latteri's co-defendant, Roskin-Frazee, used that access to fraudulently obtain at least $117,260.66 in COMPANY A merchandise and service contracts. *See* ¶ 2, Plea Agreement, *United States v. Roskin-Frazee*, No. 23-471 WHO. Additionally, during the intrusion, this

access was used to fraudulently obtain and redeem $2,727,075.37 in COMPANY A gift cards, although there is no evidence that Mr. Latteri personally benefited from either the hardware or the gift cards.

II. The Offense Was Just One Part of a Lengthy Internet Crime Spree That Involved Cyberstalking, Sextortion, Threats, and Other Serious Internet-Involved Crimes (*Defendant's History and Characteristics--18 U.S.C. § 3553(a)(1)*)

A. The defendant engaged in a years-long campaign to cyberstalk and sextort young women and others, and much of it took place *after* the charged conduct.

1. IC3 Complaints

While the FBI was investigating the intrusion into COMPANY B, agents quickly learned of Latteri's other exploits on the internet. Between 2009 and 2018, there were at least 12 different reports to the FBI's Internet Crime Complaint Center about Latteri. That's an astonishing number; most people do not report crime of this sort, and certainly not to the FBI. That suggests that the real number of victims is much higher. The reports reflected that Latteri used the Internet to serve as a one man crime spree. In August 2013, one victim told of Latteri's constant harassment and threats to users on his website. He then reported that Latteri had placed child pornography on the website in order to maliciously cause it to be taken down. *See* Aff. of Special Agent Brian Walsh in Supp. of an App. for a Search Warrant, Case No. 1:20mj3169 (N.D. Ohio Jul 10. 2020), attached as Ex. A, at 56-57 (hereinafter, "Walsh Aff."). The same victim reported that Latteri had SIM swapped him (*see infra*) to compromise his Apple iCloud account. Walsh Aff. ¶ 147. On August 12, 2015, an individual complained that Latteri's website lambos.org posted personally identifiable information, including social security numbers, addresses, banking information, and medical information about a number of people. *Id.* ¶ 148. Posting personal information of individuals online as an act of revenge or as a means of encouraging people to take action against them is often referred to as "doxing."

In May 2018, a victim complained that someone had stolen the passwords to his AOL, Yahoo, and Snapchat accounts. The FBI was able to trace the IP address of the perpetrator to Latteri. *Id.* ¶ 149. On May 17, 2019, an 18 year-old victim from Southern California complained that Latteri had been

harassing them since they were 13 or 14 years old. Latteri would hack the 13 or 14 year old's Facebook account and make threats like "I know where you live."

2. Social Engineering

Latteri used social engineering to obtain access to victims' personal accounts. In one account Latteri controlled, the FBI uncovered evidence that Latteri impersonated representatives of companies like Snapchat, Apple, and Verizon to approximately 371 different victims. Below are just a few examples of Latteri's online activity. *Id.* at 29-30.

In January 2019, Latteri appears to have gone after a particular victim by first searching for their MySpace password online and then attempting to identify their e-mail address and phone number. On January 30, 2019, after obtaining access to the user's Snapchat account, Latteri impersonated Snapchat customer service and successfully obtained the user's multifactor authentication code and attempted to obtain their My Eyes Only code.[2] *See id.* at 31 –33.

In January 2020, through a series of text messages using social engineering, Latteri gained access to a teenager's Snapchat account and also gained access to her "My Eyes Only" space. Once the victim realized Latteri had tricked her into giving him access to her most private media, she became angry: "can you please give me my account back . . . . i'm a . . . 17 year old girl idk what you're going to do with it . . . . if you don't give my account back in the next 12 hours I will file a police report on you for trying to obtain nude photos of an underage girl." *Id.* at 36 –38.

In February 2020, Latteri obtained access to another user's Snapchat account and again tried to obtain their My Eyes Only code. *See id.* at 35-36. He did the same with other victims in April 2019 and March 2020. *See id.* 38–40.

[2] The Snapchat social media platform has a feature called "My Eyes Only" that is for images that a user wants to keep "extra private"—often intimate pictures—and is set to have a special passcode that is different than the user's Snapchat password.

3. The Defendant Coerced Minors to Create and Provide Him Nude Images

Beginning in 2015, the defendant began to harass one particular victim after apparently gaining access to her computer and her accounts. He told her that if she continued to ignore him, he would put up posts on her social media accounts and email her teachers. *Id.* ¶ 142. He continued to press, asking if the victim wanted to save her life or not, and then saying that "I will stop and leave you alone forever if you give me what I want." *Id.* What Latteri wanted was "nudes." Latteri told her, "we can do this the easy way or the hard way." When Latteri found out this victim tried to report him to authorities, he mocked her. *See id.* at 52, 53.

He continued to press: "Nudes. Since you wanted to be a little prick in the past. Ill give you 10 minutes or I press send[.] I cc'd everyone. I will also make a nice post on ur FB [Facebook]. The choice is yours." He then threatened to "DDOS" the victim, *Id.* at 53.

Latteri blackmailed this particular minor, who was 16 years old, for years. He threatened to compromise her social media accounts and tell her friends and family that she was a 'slut" unless she sent him nude photos. The victim sent approximately 10 to 15 photos to Latteri. *See id.* ¶ 143.

Latteri also stalked this victim; on at least one occasion, he obtained access to her phone's location data and sent her harassing messages about where she was. *Id.*

In January 2020—almost five years after he had initially obtained the victim's nude images and after the offense conduct in this case—the defendant threatened to "leak" her photographs. *Id.* ¶ 145.

4. CPPS.me Activity

Latteri spent a lot of time on CPPS.me—the Club Penguin Private Server, which was a server for a popular multiplayer online game where there was no filtering and no restrictions. *Id.* ¶¶ 101–102. One witness told the FBI that Latteri engaged in lots of bullying on the CPPS site. Specifically, Latteri would "attack girls who wouldn't message him back or engage in conversation. He would then find their social media accounts and harass them." *Id.* ¶ 108. The online harassment Latteri engaged in on CPPS included

> compromising social media accounts and accessing those accounts without permission, threats to conduct swatting attacks,[3] text bombing (which was described as sending a large amount of text messages in a short time), harassing calls from spoofed telephone numbers, calls from the individuals own telephone number, and creation of social media accounts in the name of the target of the harassment.

Id. ¶ 109. Latteri gained access to a 15-16 year old victim's Snapchat account—likely using the social engineering discussed above—and obtained a nude photograph, posting it on the CPPS site. *Id.*

5. Discord

Elsewhere on the Internet, on his Discord servers, the defendant bragged about his exploits. On March 20, 2019, he posted evidence of installing malware on a victim's computer. *Id.* ¶ 112. On March 21, 2019, he posted a compromising picture of a young female, stating, "I have [victim's] nudes hanging in my car like this." *Id.* ¶ 114. On May 1, 2019, he posted a racist, misogynistic, and antisemitic announcement:

> @ here YOU!! Yes, YOU!!! This is a message from the global congress of sandniggers. We are letting you know that Lambos is fully operational and ready for some asskicking and some rage with autists in 3 weeks at the Annual Egirl Purge. You know what this means, don't you? This means us, the sad lonely basement-dwelers get to let out our anger towards internet females have denied us our civil liberties. This event will be the cringiest shit you will ever see, ever worse than 9/11 (fucking jews). What are you waiting for? Spray and pray against the girls you fucking couch cuck. With dedication, SHELDON (edited).

Id. ¶ 118.

6. Threats on Twitter/X

On at least one occasion, on April 16, 2019, a victim observed Latteri make a racist comment on Twitter. The victim called him out on that comment; Latteri then threatened to hack the victim's phone. Although the victim did not take Latteri seriously at the time, the victim soon found out that he took control of her Snapchat account, and tried to take control of her phone and other social media accounts.

[3] A "swatting attack" is typically when an individual calls 911 and reports a fake, but very serious, emergency at the residence of a victim and often advises the offer that violence, weapons, or an imminent risk of death is involved. This is designed to draw a substantial law enforcement response (including a SWAT team). Swatting attacks can sometimes have tragic consequences: in 2017, a Kansas man was shot and killed by officers responding to a swatting attack; the person who made the call later pled guilty and was sentenced to 20 years in federal prison. *See* https://www.nbcnews.com/news/us-news/serial-swatter-tyler-barriss-sentenced-20-years-death-kansas-man-n978291.

She initially ignored it, but then he issued a threat: from a new number, he texted her saying "have fun in school on Monday fam ur gonna need it ;P" and then followed it with "<Named School> gonna be on ALERT." *See id.* ¶¶ 151 –152. The victim had never told Latteri the name of the University she attended.

B. The defendant forged federal court subpoenas and orders in order to unlawfully obtain information to further his exploits.

On March 30, 2020, on another Discord server, Latteri admitted to hacking a particular user's Snapchat, but mused that he needed to obtain the user's Google authentication key.[4] *Id.* ¶ 128. In order to do so, Latteri said he was going to SIM swap the victim.[5] *Id.* Latteri then mused that he was going to send a subpoena to [a cloud computing company]. *Id.* ¶ 128.

This was not just talk. Instead of serving that company, the next day, March 31, 2020 Latteri sent a forged civil subpoena *duces tecum* to Cloudflare, a San Francisco company that provides, among other things network security and domain registration services. *Id.* ¶ 130. The "subpoena," which was printed on an Administrative Office of the U.S. Courts form and purported to be issued by an attorney in a civil lawsuit in the Central District of California, appeared genuine, but of course was not. *See id.* ¶¶130 –31. The subpoena was purportedly issued by Caitlyn Delpute, an attorney for the Walt Disney Company. On April 2, 2020, Latteri sent an email from the return address "caitlyn.delpute@disney-dmca.com" in which he followed up on the subpoena and asked for a phone call. *Id.* ¶ "Caitlyn Delpute" is not a member of the California Bar but appears to be a name that Latteri made up. *Id.* ¶ 136. Latteri, apparently frustrated that he did not receive an immediate response to his fake subpoena, then falsified

[4] A Google authentication key is a form of multifactor authentication that acts as an additional layer of security when logging into one's Google account.

[5] In a "SIM Swap," the perpetrator uses social engineering or some other method to take control of the victim's cell phone account such that any text messages that are sent to the victim—in particular, two-factor authentication/one-time passcodes that are used to verify an online user's identity—are actually sent to the perpetrator.

an order purporting to be from the United States District Court for the Central District of California that ordered Cloudflare to "temporarily disable the access" of two websites. *Id.* ¶ 134.

Latteri also took a similar tack with Namecheap, another popular domain name registrar. After first pretending to be "Adam McMiller," an attorney in Disney's Legal Department and serving a "subpoena," he switched to "Delpute" before serving Namecheap with a forged court order. A redacted report of interview with Namecheap representatives and the fictious subpoena and order issued to NameCheap are attached as Exhibit B.

C. The Defendant's Criminal Conduct Continued Through Last Year

As reflected in the PSR, the defendant was most recently arrested in Ohio on January 31, 2024. He was convicted of four felony counts of forgery, which revolved around him defrauding at least three different victims. *See* PSR ¶ 34. That is further evidence that his criminal conduct did not end with this case.

III. A Custodial Sentence is Necessary for General and Specific Deterrence (*18 U.S.C. § 3553(a)(2)(B)*)

The defendant's serious crimes of conviction, coupled with his years-long cyberstalking, harassment, and exploitation activity, as well as his more recent criminal activity in Ohio, militate in favor of a custodial sentence. He has not been deterred by his previous experiences with law enforcement. Moreover, cybercrime of the sort here is particularly difficult to detect, so principles of general deterrence, too, militate in favor of a custodial sentence.

IV. The Need to Protect the Public Requires the Addition of a Special Condition Allowing Probation to Monitor the Defendant's Internet Activity (*18 U.S.C. § 3553(2)(C)*)

Following any prison term imposed, the government agrees with the probation officer that the Court should order the maximum statutory term of supervised release—three years. The government agrees that the Court should include the special conditions recommended by the probation officer, but in light of the defendant's specific history of committing substantial crimes against hundreds of victims using the Internet, and his obvious technical skill and prowess, the Court should also impose additional

conditions to allow probation to monitor Latteri's Internet use, akin to that which is typically used in child exploitation cases.

Specifically, the Court should impose the following additional special conditions:

1. You must not possess or use a computer without the prior approval of the probation officer. "Computer" includes any electronic device capable of accessing the internet or processing or storing data as described at 18 U.S.C. § 1030(e)(1) (including cell phones), and all peripheral devices.

2. As directed by the probation officer, you must enroll in the probation office's Computer and Internet Monitoring Program (CIMP) and must abide by the requirements of the CIMP program and the Acceptable Use Contract.

3. You must not access the Internet or any "on-line computer service" at any location (including employment) without the prior approval of the probation officer. "On-line services" include any Internet service provider, or any other public or private computer network. As directed by the probation officer, you must warn your employer of restrictions to your computer use.

4. You must consent to the probation officer conducting periodic unannounced examinations of your computer equipment which may include retrieval and copying of all data from your computer(s) and any peripheral device to ensure compliance with this condition, and/or removal of any such equipment for the purpose of conducting more thorough inspection. You must also consent to the installation of any hardware or software as directed by the probation officer to monitor the defendant's Internet use.

5. You must not possess or use any data encryption technique or program or any technique or software designed to anonymize your presence on the Internet, including, but not limited to, the use of virtual private networks or the Tor browser.

The Court has broad discretion to impose conditions of supervised release where they are reasonably related to the statutory sentencing factors. *United States v. Riley*, 576 F.3d 1046, 1048 (9th Cir. 2009). *Accord* Judgment, *United States v. Bell*, Case No. 17-CR-475 (N.D. Cal. Oct. 12, 2018) (Breyer, J.) (imposing identical conditions in the case of defendant who purchased carfentanil on dark web).

V. Restitution

Pursuant to 18 U.S.C. § 3663A, restitution must be ordered as part of any judgment in this case. Mr. Latteri has agreed that he owes at least $3,827,835.66 to COMPANY B, which represents the total of COMPANY B's incident response costs, and the government requests that the Court order him to pay that amount, jointly and severally, with Mr. Roskin-Frazee.

Additionally, the government received notice just today that COMPANY A is requesting $506,694.98 in restitution for incident response costs, and would request that the Court order that as well. *See* Declaration of Alejandro Marti Minguez, attached as Exhibit C. In sum, the government requests the Court order restitution as follows:

COMPANY A	$506,694.98
COMPANY B	$3,827,835.66

VI. Conclusion

For the foregoing reasons, the Court should impose a custodial sentence of 36 months, followed by a three year term of supervised release subject to the terms and conditions described above, and restitution as set forth above.

Dated: April 24, 2025

Respectfully submitted,

MARTHA BOERSCH
Attorney for the United States
Acting under Authority Conferred by 28 U.S.C. § 515

By: _____/s/_____
NIKHIL BHAGAT
Assistant United States Attorney